



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/870,411	05/29/2001	Brian Andrew	1215	8015

7590 02/03/2005

MICHALIK & WYLIE PLLC  
704 - 228th Avenue NE  
Suite 193  
Sammamish, WA 98074

EXAMINER
----------

DERWICH, KRISTIN M

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 02/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/870,411

Applicant(s)

ANDREW ET AL.

Examiner

Kristin Derwich

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 5/29/01.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 1-24 is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 May 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 2/11/03.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## DETAILED ACTION

1. Claims 1-24 pending.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 1 recites the limitation "the installable software component" in lines 14-15 and lines 26-27. There is insufficient antecedent basis for this limitation in the claim. Although an interchangeable cryptographic module was mentioned it is not clear whether the "installable software component" is referring to the same thing.

### ***Double Patenting***

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Omum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Art Unit: 2132

3. Claims 1-24 rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-58 of U.S. Patent No. 6,249,866 in view of Kaplan et al. (Kaplan), U.S. Patent No. 6,704,871.

4. As per claims 1-3, 5 and 6:

Claim 1 of U.S. Patent No. 6,249,866 discloses a computer system having a file system, a method of encrypting or decrypting data in a file stored in a non-volatile storage, comprising:

receiving information at the file system indicating that the file is designated as encrypted;

receiving an encryption key associated with the file;

receiving a request to write file data to non-volatile storage and receiving the file data, and in response, encrypting the file data into encrypted file data at file system level software using the encryption key, writing the encrypted file data to non-volatile storage and writing encryption key information in association with the file to the same non-volatile storage as the encrypted file data; and

receiving a request to read file data from non-volatile storage, and in response, reading the encrypted file data from the non-volatile storage, decrypting the encrypted file data into decrypted file data at the file system level software using the encryption key, and returning the decrypted file data (col 19, lines 29-49);

The system of claim 1 differs from claim 1 of the instant application in that it does not utilize an interchangeable cryptographic module to supply a plurality of cryptographic algorithms to the file system level software.

However, Kaplan, in an analogous environment, discloses a cryptographic co-processor that can be substituted for a regular processor with little modification to the existing product (col 2, lines 40-45). This makes it interchangeable between a regular processor and a cryptographic co-processor. This co-processor provides a library of various cryptographic and encryption algorithms or functions (col 6, lines 61-65). The existence of the library removes the need to recreate any encryption, hashing or public key algorithms (col 7, lines 3-6). In addition, because the co-processor is interchangeable, a different cryptographic co-processor could be substituted with a different library set of cryptographic algorithms.

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to incorporate the teachings of Kaplan into the system of U.S. Patent No. 6,249,866 to provide for an interchangeable cryptographic module. This modification would have been obvious because one of ordinary skill in the art would have wanted to make the system more flexible as new cryptographic techniques became available. Instead of having to change the entire system, only a new cryptographic processor or module would be needed. This would also be more cost effective.

5. The system of claim 1 differs from claim 2 of the instant application in that it fails to teach the system level software specifying a selected algorithm to use.

However, Kaplan discloses commands that can be used to access the library containing a plurality of cryptographic algorithms in order to select the desired algorithm (col 7, lines 1-3). Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to incorporate a method of choosing a desired algorithm out of a plurality because the system would need a way of intelligently selecting a single algorithm out of the multiple available since the algorithm would need to be able to decrypt as well as encrypt.

6. The system of claim 1 differs from claim 3 of the instant application in that it fails to teach the system level software specifying the algorithm to use by calling a corresponding function.

However, Kaplan discloses functions in the form of pre-programmed commands that correspond to the various algorithms (col 7, lines 8-11). Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to utilize functions that correspond to the algorithms as a means of selection because this would allow any pre-processing to occur before calling the algorithm. If the algorithm required certain variables to be initialized with certain values, or if metadata needed to be extracted before calling the algorithm, a command or function would be able to accomplish these tasks before executing the actual algorithm.

7. The system of claim 1 differs from claim 5 of the instant application in that fails to teach an interchangeable cryptographic module registering functions with the file system level software.

However, Kaplan discloses the commands previously mentioned being recognized by the co-processor that accesses the library of algorithms (col 7, lines 18-22). Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to have the functions corresponding to the algorithms be recognized by the entity choosing the desired algorithm. If the functions were not registered and could not be recognized by the deciding entity then the algorithm corresponding to the unrecognizable and unregistered function could not be called.

8. The system of claim 1 differs from claim 6 of the instant application in that it fails to teach the interchangeable cryptographic module and file system level software as kernel mode components.

However, Kaplan discloses the choice of a kernel mode for the cryptographic co-processor (col 6, lines 28-32). Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to make the cryptographic module and file system level software kernel mode components because it would make the entire process run faster and provide an extra layer of protection against attack.

9. As per claim 4:

Claim 13 of U.S. Patent No. 6,249,866 discloses a method of encrypting and decrypting data comprising placing a callout to a run-time library of software functions (col 20, lines 28-30).

The system of claim 13 differs from claim 4 of the instant application in that it fails to teach the system level software sending a callout to the interchangeable cryptographic module indicating whether encryption or decryption is needed.

However, Kaplan discloses a cryptographic co-processor that will dedicate cryptographic resources to encryption and decryption requests when indicated (col 2, lines 19-22). Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to have some sort of method in place to indicate whether or not the cryptographic module needed to encrypt or decrypt. This would have been important because the cryptographic module would need a way to tell what type of data was being processed and whether it needed to be encrypted or decrypted so as not to encrypt or decrypt something twice.

10. As per claims 7 and 9:

Claim 14 of U.S. Patent No. 6,249,866 discloses a method of reading unencrypted file data or encrypted file data and returning the data read as unencrypted file data, comprising, receiving at the file system from a requesting program a request to read file data from a non-volatile storage, reading the file data, determining at file system software if the file data is encrypted, and if the file data is not encrypted, returning the file data to the requesting program, and if the file data is encrypted, obtaining a file encryption key for that file by applying a private key to the file encryption key data, the file encryption key data including the file encryption key encrypted with a public key and stored on the same non-volatile storage and in association with the file, providing the file encryption key and the file data to a file system level decryption mechanism, decrypting the file data into unencrypted file data, and returning the unencrypted file data to the requesting program.



The method of claim 14 differs from claim 7 of the instant application in that the file system software does not communicate with an interchangeable cryptographic module that supplies a plurality of selectable cryptographic algorithms.

However, Kaplan, in an analogous environment, discloses a cryptographic co-processor that can be substituted for a regular processor with little modification to the existing product (col 2, lines 40-45). This makes it interchangeable between a regular processor and a cryptographic co-processor. This co-processor provides a library of various cryptographic and encryption algorithms or functions (col 6, lines 61-65). The existence of the library removes the need to recreate any encryption, hashing or public key algorithms (col 7, lines 3-6). In addition, because the co-processor is interchangeable, a different cryptographic co-processor could be substituted with a different library set of cryptographic algorithms.

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to incorporate the teachings of Kaplan into the system of U.S. Patent No. 6,249,866 to provide for an interchangeable cryptographic module. This modification would have been obvious because one of ordinary skill in the art would have wanted to make the system more flexible as new cryptographic techniques became available. Instead of having to change the entire system, only a new cryptographic processor or module would be needed. This would also be more cost effective.

Art Unit: 2132

11. The method of claim 14 differs from claim 9 of the instant application in that the file system level software doesn't invoke the algorithm of the cryptographic module by calling a function with input buffer, output buffer and key-related data.

However, Kaplan discloses functions in the form of pre-programmed commands that correspond to the various algorithms on the cryptographic co-processor which is electronically linked to a processing unit which contains input and output capabilities along with a master key used for cryptographic processes (col 7, lines 8-11; col 186, lines 32-39). Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to utilize functions that correspond to the algorithms as a means of selection because this would allow any pre-processing to occur before calling the algorithm. If the algorithm called for variables to be initialized with certain values, or if certain metadata needed to be extracted before calling the algorithm, a command or function would accomplish these tasks before executing the actual algorithm.

12. Claim 8 of the instant application is rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 45 of U.S. Patent No. 6,249,866. Although the conflicting claims are not identical, they are not patentably distinct from each other because the scope is the same between the two. Both are reading algorithm data associated with the encrypted file data. This would have been obvious to one of ordinary skill in the art because if the algorithm data were not stored with the encrypted file data then it would have taken more time and complexity to map the algorithm data that identified the algorithm used in conjunction with the encrypted file data.

Art Unit: 2132

13. As per claim 10, this claim is directed to a computer readable medium having computer-executable instructions for performing the method of the instant application wherein such a medium is also claimed in U.S. Patent No. 6,249,866 at claim 46.

Accordingly, such claimed limitations also would have been obvious over U.S. Patent No. 6,249,866 in view of Kaplan, as noted above.

14. As per claim 19 and 22:

Claim 24 of U.S. Patent No. 6,249,866 discloses a computer system having a file system, a system for encrypting data written by the file system to a non-volatile storage, comprising, means for obtaining a file encryption key, a software encryption mechanism at a file system software level for converting unencrypted data to encrypted data based on the file encryption key, the file system writing at least some of the data as encrypted data to a file in the non-volatile storage, and means for encrypting the file encryption key, the file system writing the encrypted file encryption key to the same nonvolatile storage as the encrypted data and in association therewith.

The method of claim 24 differs from claim 19 of the instant application in that the file system software does not communicate with an interchangeable cryptographic module that supplies a plurality of selectable cryptographic algorithms.

However, Kaplan, in an analogous environment, discloses a cryptographic co-processor that can be substituted for a regular processor with little modification to the existing product (col 2, lines 40-45). This makes it interchangeable between a regular processor and a cryptographic co-processor. This co-processor provides a library of various cryptographic and encryption algorithms or functions (col 6, lines 61-65). The

Art Unit: 2132

existence of the library removes the need to recreate any encryption, hashing or public key algorithms (col 7, lines 3-6). In addition, because the co-processor is interchangeable, a different cryptographic co-processor could be substituted with a different library set of cryptographic algorithms.

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to incorporate the teachings of Kaplan into the system of U.S. Patent No. 6,249,866 to provide for an interchangeable cryptographic module. This modification would have been obvious because one of ordinary skill in the art would have wanted to make the system more flexible as new cryptographic techniques became available. Instead of having to change the entire system, only a new cryptographic processor or module would be needed. This would also be more cost effective.

15. The method of claim 24 differs from claim 22 of the instant application in that it fails to teach the system level software specifying the algorithm to use by calling a corresponding function.

However, Kaplan discloses functions in the form of pre-programmed commands that correspond to the various algorithms (col 7, lines 8-11). Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to utilize functions that correspond to the algorithms as a means of selection because this would allow any pre-processing to occur before calling the algorithm. If the algorithm needed certain values to be initialized a certain way, or if certain metadata needed to be

extracted before calling the algorithm, a command or function would be able to accomplish these tasks before executing the actual algorithm.

16. Claims 20 and 21 of the instant application are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 48 and 50 of U.S. Patent No. 6,249,866. Although the conflicting claims are not identical, they are not patentably distinct from each other because their basic scope in function is the same. Both are writing information identifying a selected algorithm to the non-volatile storage in association with the encrypted file. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to write this identification information in association with the encrypted file in order to make it easier to locate. Making the information readily available for reading in association with the encrypted file saves time and money when trying to decrypt the file.

17. As per claim 23 and 24:

Claim 56 of U.S. Patent No. 6,249,866 discloses a computer system having a file system, a method of returning requested file data, comprising:

receiving at file system software a request to read file data of an encrypted file;

determining whether file data corresponding to the request is stored on a storage medium or has been decrypted to an access-controlled location; and

if the file data has been decrypted to the access-controlled location, returning the file data in decrypted form from the access-controlled location in response to the request; or

if the file data is stored on the storage medium, reading the file data corresponding to the request from the storage medium, decrypting the file data at the file system software into unencrypted file data, and returning the unencrypted file data in response to the request.

The method of claim 56 differs from claim 23 of the instant application in that the file system software does not communicate with an interchangeable cryptographic module that supplies a plurality of selectable cryptographic algorithms.

However, Kaplan, in an analogous environment, discloses a cryptographic co-processor that can be substituted for a regular processor with little modification to the existing product (col 2, lines 40-45). This makes it interchangeable between a regular processor and a cryptographic co-processor. This co-processor provides a library of various cryptographic and encryption algorithms or functions (col 6, lines 61-65). The existence of the library removes the need to recreate any encryption, hashing or public key algorithms (col 7, lines 3-6). In addition, because the co-processor is interchangeable, a different cryptographic co-processor could be substituted with a different library set of cryptographic algorithms.

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to incorporate the teachings of Kaplan into the system of U.S. Patent No. 6,249,866 to provide for an interchangeable cryptographic module. This modification would have been obvious because one of ordinary skill in the art would have wanted to make the system more flexible as new cryptographic techniques became available. Instead of having to change the entire system, only a new

Art Unit: 2132

cryptographic processor or module would be needed. This would also be more cost effective.

The method of claim 56 differs from claim 24 of the instant application in that it fails to teach the system level software specifying the algorithm to use by calling a corresponding function.

However, Kaplan discloses functions in the form of pre-programmed commands that correspond to the various algorithms (col 7, lines 8-11). Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to utilize functions that correspond to the algorithms as a means of selection because this would allow any pre-processing to occur before calling the algorithm. If the algorithm needed certain values to be initialized a certain way, or if certain metadata needed to be extracted before calling the algorithm, a command or function would be able to accomplish these tasks before executing the actual algorithm.

18. Claims 1, 14, 22, 25, 33-34, 38 and 46 of U.S. Patent No. 6,249,866 contain every element of claims 11-15, 17 and 18 of the instant application and as such anticipate claims 11-15, 17 and 18 of the instant application.

"A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim. In re Longi, 759 F .2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F .3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a

Art Unit: 2132

patent claim to a species within that genus)." ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

19. Claim 16 is rejected as being unpatentable over U.S. Patent No. 6,249,866 as applied to claim 11 above and further in view of Kaplan.

U.S. Patent No. 6,249,866 fails to teach an algorithm component separate from the file system level component that provides at least one algorithm for performing encryption and decryption operations. However, Kaplan discloses a separate library of cryptographic algorithms (col 6, lines 61-65).

It would have been obvious to one of ordinary skill in the art, at the time of the invention, to have a separate algorithm component comprising at least one algorithm for performing encryption and decryption because having a separate algorithm component would have allowed for flexibility. As new algorithms became available they could be added to the component without having to replace the entire file system software which would also save money.

### ***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.



Art Unit: 2132

U.S. Patent No. 6,185,681 (Zizzi) discloses a cryptographic software module being added to an electronic document management system which transparently encrypts or decrypts the documents similar to the instant invention.

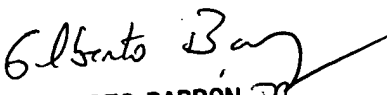
"Microsoft Kernel Cryptographic Module" describes an interchangeable, kernel component, cryptographic module similar to the instant invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KD  
\*\*\*

  
GILBERTO BARRON JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100